19801 SW 72nd Ave.
Suite 250
Tualatin, Oregon 97062

(503) 885-9699

Digimarc Corporation

DIG35 Metadata and Digital Watermarking

Strengthening Digital Image Metadata with Digital Watermarks

Version 0.8

Date: ***February 17, 2000***

Digimarc Confidential

APPENDIX A

Table of Contents

Metadata and Digital Watermarking

By combining the DIG35 metadata standard, digital watermarking, and asset management technologies, the flexibility, persistence and accuracy of image metadata can be enhanced.

Overview

Low cost digital cameras and scanners, film to CD processing, and photo sharing web-sites are all helping fuel an explosive growth in digital imaging; a growth that both creates new opportunities for digital imaging and that brings with it new management problems. Whether you are a home enthusiast or a professional in the imaging industry, dealing with the sheer number of digital images is becoming a major problem. Fortunately, digital images, unlike their paper counterparts, can be part of the solution to the management problem.

By combining the digital image with other data about that image -- i.e. image owner, location where the image was taken, and date and time when the image was taken -- we can develop applications and processes to manage the flood of digital images. Such additional information is referred to as *metadata*, or data about data. Digital images allow data to be embedded directly into an image, giving them a distinct advantage over paper images.

Some tools such as Asset Management Systems and Workflow Applications try to address the management issues involved with digital imaging. These tools store metadata; in some form and in some location. But these systems are proprietary and do not enable the metadata gathered about an image in one device or application to be used in another device or application. In order to create devices, applications and processes that effectively and efficiently use metadata, they must all agree on the form of the metadata.

The Digital Imaging Group's (DIG) DIG35 Initiative, building upon the XML (eXtensible Markup Language) standard, specifies the syntax and semantics of one such imaging metadata standard. This standard will enable different imaging devices, applications and processes to seamlessly work together. Additional work is being done by the <indecs> project and the DOI Initiative to extend this interoperability beyond the imaging industry. By defining metadata frameworks and object identification, an infrastructure can be defined that will enable unprecedented levels of sharing and management of intellectual property. The remainder of this paper will focus on the DIG35 Initiative and the image industry, but by extension, can be applied to other industries as well.

While the DIG35 metadata standard provides a foundation for future development, real world issues cause problems with deployment today. Non-compliant image formats, imaging applications and devices, all contribute to weakening the reliability of imaging metadata. Either through unintentional, unavoidable or malicious usage, image metadata can be lost or altered. Additionally, there are situations where it may not be advantageous or proper to store the metadata with the image itself. One solution to these situations is to store the metadata in a separate repository, a metadata server, and store a unique link within the image that references back to the separately stored metadata.

The remaining problem with this solution is that the link within the image cannot itself be metadata. That is, the link needs to be part of the image, and not any extraneous information. (As we saw above, any extraneous information can be lost or modified.) Digital watermarking solves this problem by embedding a digital watermark directly into the image. Such a watermark uniquely identifies each image, and hence, provides the needed reference back to the metadata.

DIG35 Metadata Standard

The vision for the DIG35 Initiative Group is to "provide a standardized mechanism which allows end-users to see digital image use as being equally as easy, as convenient and as flexible as the traditional photographic methods while enabling additional benefits that are possible only with a digital format."

The DIG35 Initiative Group has chosen to employ the W3C's Extensible Markup Language (XML) as the recommended mechanism to provide image metadata. The reasons for choosing XML include:

- adoption in Internet enabled applications;
- cross-platform nature;
- extensibility;
- device and operating system independence; and,
- human and machine readable format.

The DIG35 Initiative Group then layers image metadata semantics on the XML underpinnings. This enables different image related applications (i.e. workflow, asset management, image capture) to effectively work together.

For example, consider an insurance company that processes auto accident claims; claims that include images. These images may be acquired by digital cameras or scanners. As the claim (with images) goes through the claims approval process, these images may be modified by a number of different image editing applications on a number of different computing platforms. And throughout, the claims processing application will be manipulating the image metadata. In order to use the same metadata from the beginning of the claims approval process to the end, each device and application in the process must understand the format and meaning of the metadata.

XML provides the means for understanding the format of the metadata, so it allows each application to read the metadata. But, it does not address the *meaning*, or semantics, of the metadata. For example, the digital camera may add date and time information about when the image was taken, the claims processing application may add date and time information about when the claim was processed, and the image editing application may add date and time information about when the image was edited. Without a standard that specifies the meaning of each, information may be lost or corrupted. The DIG35 Initiative supplies the needed meaning to the metadata.

Vulnerability of Metadata

As valuable as this image metadata is, it is also extremely vulnerable. First, DIG35 compliant image metadata relies on new and evolving image formats. Until such time as all imaging applications, processes and devices are upgraded to support the latest image formats in a sympathetic manner, DIG35 metadata is vulnerable to accidental deletion or to unavoidable loss. Such vulnerabilities include:

- Workflows where an image is converted to a non-DIG35 compliant image format and hence, loses the image metadata;
- Imaging applications that don't preserve metadata during image manipulation (see Figure 1); and,
- Converting a digital image to a non-digital format and subsequently, back to a digital format (e.g., printing out an image and then scanning it back in).
- Preparing an image for the WWW where file size and download time need to be minimized.

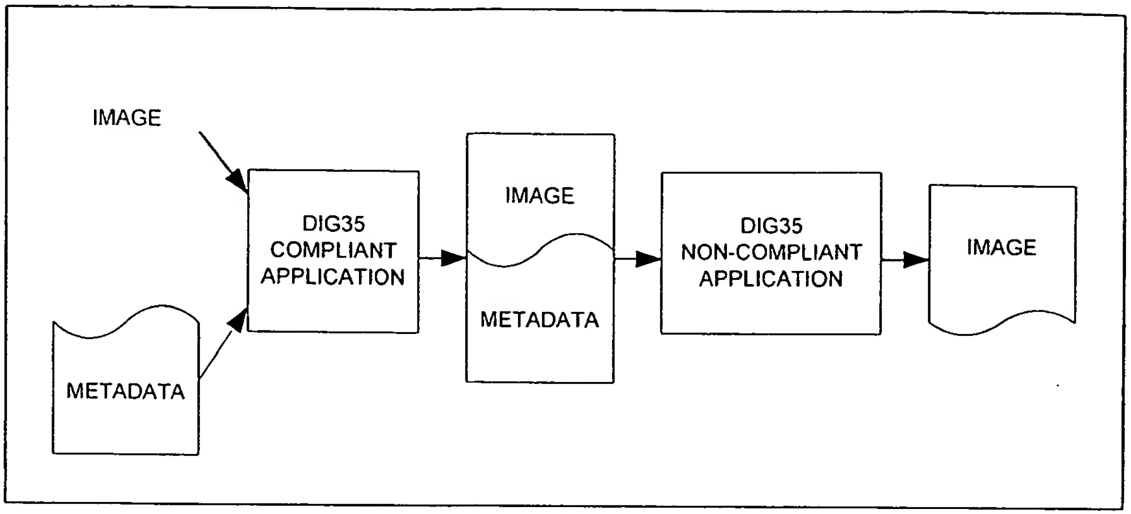

Figure 1

A DIG35 Compliant application adds metadata to an image, only to have that metadata lost when the image is processed by a non-compliant application.

Let's return to our example of the auto insurance company. Digital images are taken by the insurance agents and incorporated into the claim. A claims adjuster then processes this claim. Finally, a claims manager approves the claim. During this processing, the image may be moved from one computer platform to another (from a PC to a Unix Server to a Macintosh). For various reasons, the image may change from one format to another as it progresses from one computer to another (BMP to TIFF to JPEG). During each of these format changes, metadata may be lost if each image converter and each image format is not DIG35 compliant. The image may also be altered to facilitate its processing by adjusting its size or by converting to grayscale. During each of these alterations, metadata may again be lost if the image processing application is not DIG35 compliant. Finally, if the final claim is printed or faxed, all of the image metadata will be lost.

The second image metadata vulnerability is malicious deletion or modification of the image metadata. By its nature, XML is stored as plain text. This makes it very easy to either change or delete the embedded image metadata. (Of particular note is the vulnerability of copyright information. With traditional film, one could assert a copyright by possession of the negative. However, with digital photography, there is no negative and hence, copyright enforcement requires new tools and techniques.)

Digital watermarking helps address both of these types of vulnerabilities. By uniquely identifying each image, a link can be established and maintained between the image and its metadata. This enables tracking and asset management of images and interoperability between DIG35 devices and applications even when the embedded metadata has been lost or changed.

Persistent Digital Watermarks and Metadata Servers

Since a digital watermark is embedded into the image data itself, the watermark cannot easily be changed or deleted without degrading the digital image. This enables a persistent link between image and metadata. By utilizing digital watermarks that uniquely identify images and storing DIG35 image metadata in a separate metadata server, an image can always be identified and its image metadata retrieved, even when using non-DIG35 compliant applications or image formats.

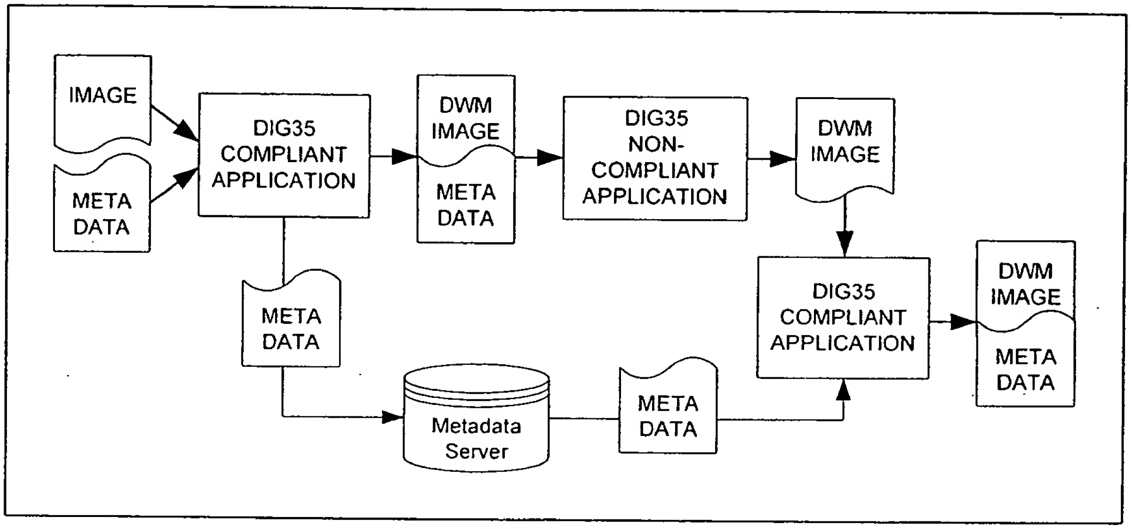

Figure 2

A DIG35 Compliant application adds metadata to an image and stores it with a metadata server. The metadata is lost when the image is processed by a non-compliant application, but is restored by a compliant application that retrieves the metadata from the metadata server.

Continuing with our earlier example of auto insurance claims processing. When the image is first acquired, it is digitally watermarked and the metadata is copied to a metadata server. The image is originally saved in TIFF format on an IBM compatible PC. To support an Intranet based application, the image is subsequently converted to JPG and stored on a UNIX Web Server. In doing so, the embedded metadata is lost. Now, even though the image has been processed and the embedded metadata has been lost, users can still retrieve the associated metadata data from the metadata server by using the digital watermark found in the image itself.

This concept can be extended beyond a single system by adding another component, the *metadata router*. The metadata router is used by an application to route a request for metadata to a remote metadata server. Assume a collection of different and distributed systems, each with its own metadata server. An application can request metadata about any image, without knowing which metadata server has that metadata. The application makes this request by requesting the data from the metadata router. The router, using the identifying information in the watermark, can redirect the request to the appropriate metadata server.

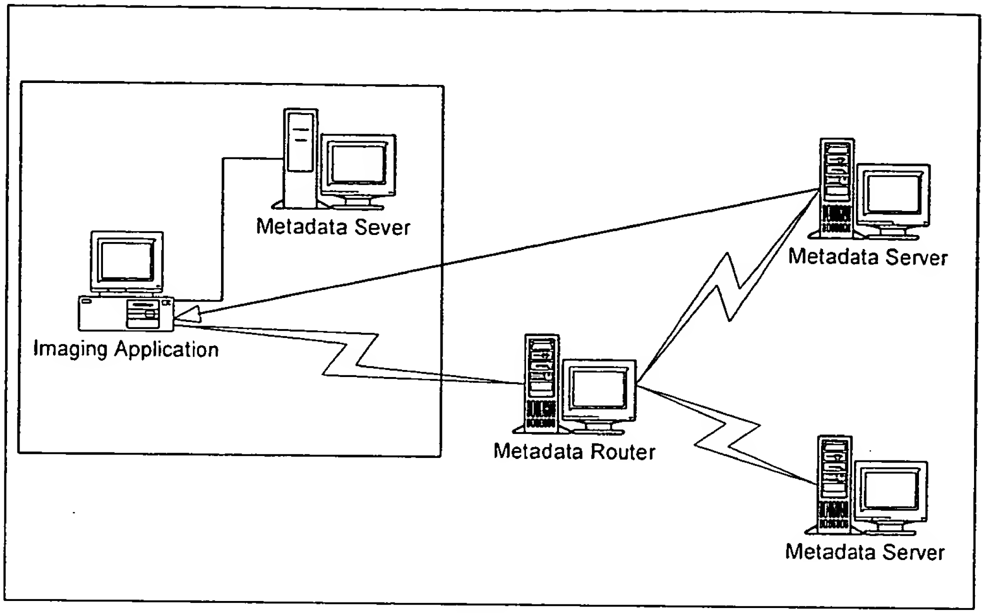

Figure 3:

An Imaging Application requests metadata from the local Metadata Server, which forwards the request, via the Metadata Router, to an another Metadata Server.

Finishing with our friendly auto insurance company, let's assume that there are a number of branch offices. Branch Office A begins a processes a claim, and storing all the image metadata on the local metadata server. Later, Branch Office B needs to do some additional work on the claim. During processing, they have occasion to need to access the metadata about a particular image. The application makes a request to the metadata router, where the router redirects the request to the metadata server at Branch Office A. The server there returns the requested metadata.

Summary

While the rapid advances in digital imaging are opening up wonderful new possibilities for using digital images, it is imperative that we utilize new tools in the management and control of these digital images. The DIG35 Initiative provides a roadmap for future developments surrounding metadata enhanced digital imaging.

To be useful, the metadata must be reliable. Today, with non-compliant applications and devices, the metadata cannot easily be integrated into existing processes, if at all. Additionally, due to file size or confidentiality concerns, it may not be desirable or proper to embed metadata directly into the image itself. By combining the DIG35 Metadata Standard, digital watermarking and metadata servers, it is possible to greatly increase the reliability and usability of image metadata.

Further, by utilizing a metadata router, the reach of the metadata system is greatly increased. In addition to knowing metadata about images within its own system, the metadata server can discover information about images from other systems.